

AMENDMENTS TO THE DRAWINGS:

The attached sheets of drawings includes changes to Figures 4 and 5. Figures 4 and 5 have been amended to eliminate the beginning preposition "TO" from steps 401, 406, 407, and 502.

REMARKS

The application has been amended and is believed to be in condition for allowance.

Claims 1-15 previously pending have been cancelled and replaced with new claims 16-23.

The Official Action objected to the drawing figures due to the introductory preposition "TO".

Responsively, the drawing figures have been amended to remove the preposition "TO" from steps 401, 406, and 407 of Figure 4 and to remove the preposition "TO" from step 502 of Figure 5. Withdrawal of the drawing objection is solicited.

The Official Action objected to the abstract and specification.

Responsively, the abstract and specification have been amended. Withdrawal of this objection is therefore solicited.

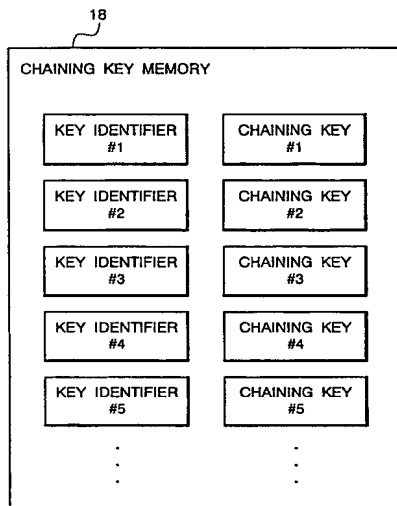
The Official Action objected to the previously-pending claims due to various informalities. The Official Action rejected claims 2-15 under 112, second paragraph, as indefinite.

The new claims have been drafted taking into account these formal criticisms and to recite the invention in a definite manner. Accordingly, withdrawal of the indefiniteness rejection is solicited.

Claims 1-15 stand rejected as anticipated by SATO 6,219,422.

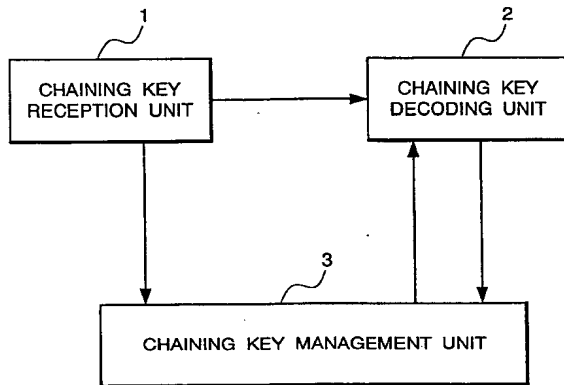
As an initial matter, the invention will be reviewed. Reference is first made to Figure 3 which illustrates a chaining key memory (18) storing plural key identifier-chaining key pairs (a series of pairs), each stored key identifier-chaining key pair comprising a key identifier and a corresponding chaining key.

FIG. 3



With reference to Figure 1, the invention comprises a chaining key broadcasting reception system, having a chaining key decoding unit 1, a chaining key management unit 3 in bi-directional communication with the chaining key decoding unit 2. The chaining key management unit stores the chaining keys of Figure 3.

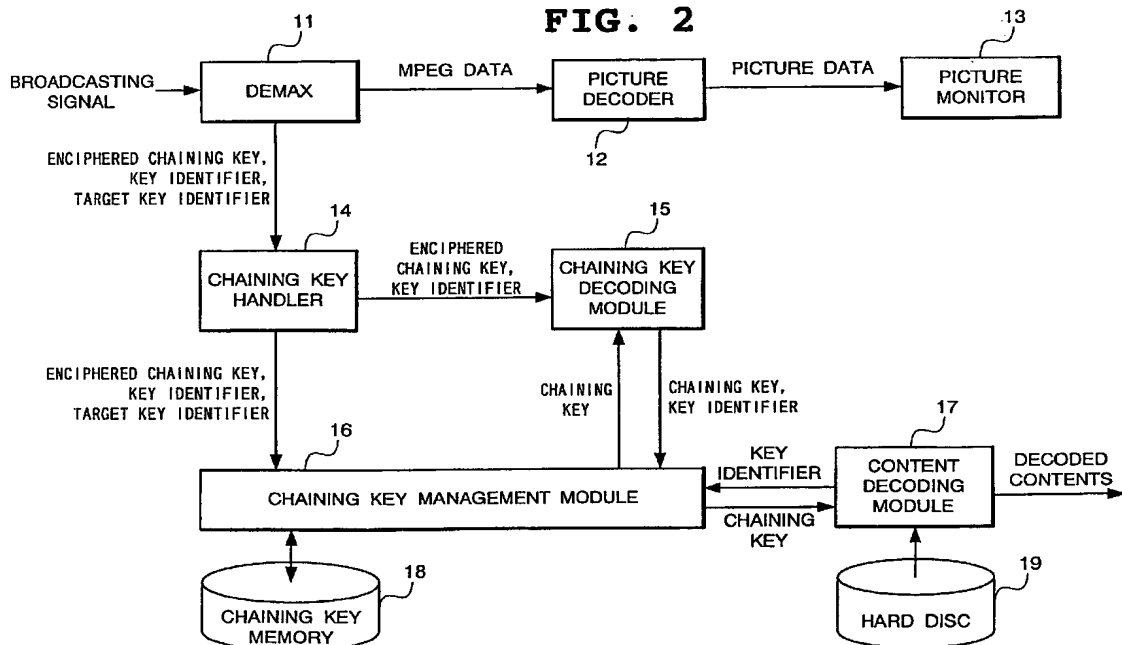
FIG. 1



The chaining key management unit is configured to retrieve a stored chaining key as determined by a target key identifier and then send the retrieved chaining key to the chaining key decoding unit.

Figure 2 is a block diagram of the invention.

FIG. 2



As illustrated, a demux 11 has a broadcast signal input and a data output and a key output. The demux is configured to receive a digital broadcast signal at the broadcast signal input and i) at the data output, to output separated digital broadcasting signal into data comprising picture and voice, and ii) at the key output, to output the enciphered chaining key, the key identifier, and the target key identifier.

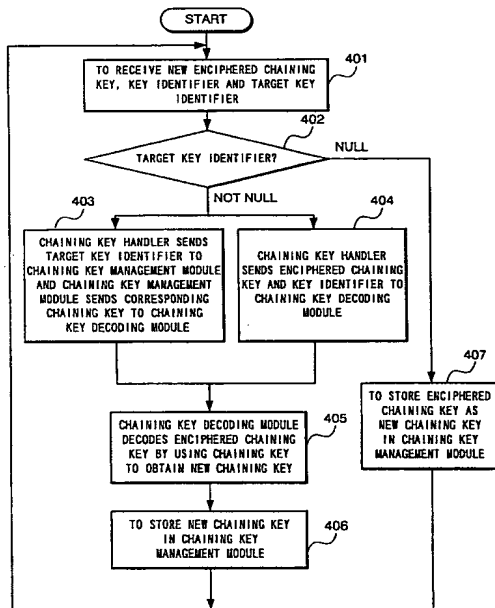
There is also provided a picture decoder 12 connected to the data output of the demux and providing an output picture data to a picture monitor 13, the picture decoder configured to decode the picture and voice to generate picture data for display on the monitor.

New claim 18 recites i) a chaining key handler 14 with a first key handler output (right side of block 14) and a second key handler output (bottom side of block 14); ii) a chaining key decoding module 15 connected to the first key handler output; and a chaining key management module 16 in bi-directional communication with the chaining key decoding module and connected to the second key handler output.

A content decoding module 17 is recited as being in bi-directional communication with the chaining key management module and with a decoded contents output. The chaining key memory 18 is in bi-directional communication with the chaining key management module.

With reference to Figure 4, the execution of the invention is illustrated.

FIG. 4



At step 401, a chaining key, a key identifier, and a target key identifier may be applied to the chaining key handler 14. However, note that the target key identifier may be null or non-null.

The chaining key handler 14 determines if target key identifier null or non-null at step 402.

When the target key identifier is null (step 402 right side branch), the chaining key handler sends the key identifier and a chaining key to the chaining key management module 16, so that the chaining key management module 16 pairs key identifier and the chaining key, as a first pair, and then stores the first

pair in the chaining key memory 18 (Step 407).

Figure A (attached) shows the processing in the first transmission when the target key identifier is null. Figure B shows the processing after the second transmission, when the target key identifier is non-null. Figure C shows an example of the second transmission, using specific chaining keys, key identifiers and target key identifiers.

Returning to step 402, when the target key identifier is non-null (indicating an encoded first chaining key has been received), the chaining key handler 14 obtains a new chaining key, from the enciphered chaining key, so that the chaining key management module 16 can store the obtained new chaining key in the chaining key memory 18 (Step 406).

To obtain a new chaining key from the enciphered chaining key, steps 403 and 404 are involved.

At step 403, the chaining key handler 14 first sends the target key identifier to the chaining key management module 16 and the chaining key management module 16 sends a chaining key paired with the target key identifier to the chaining key decoding module 15.

At step 404, the chaining key handler 14 sends the key identifier and the enciphered chaining key to the chaining key decoding module 15.

At step 405, the chaining key decoding module 15 decodes the enciphered chaining key (received from by the

chaining key handler 14) with the chaining key obtained from the chaining key management module 16 to thereby obtain a new chaining key.

The chaining key decoding module 15 sends the new chaining key and a key identifier (obtained from the chaining key management module 16) to the chaining key management module 16, so that the chaining key management module 16 stores the new chaining key and the obtained key identifier as a pair in the chaining key memory 18 (Step 406).

Figure 5 shows the enciphered contents decoded (using a chaining key) by the content decoding module 17 and the chaining key management module 16.

The content decoding module 17 designates a key identifier to take out a chaining key from the chaining key management module 16 (Step 501). The content decoding module 17 decodes the enciphered contents using the chaining key obtained from the chaining key management module 16 (Step 502). Thus, by sequentially decoding a subsequently received key with a key received at a last time, only a viewer who has viewed a program from the beginning to the end or who has viewed the whole of a serial drama (to receive all of a series of keys) is allowed to obtain a final key.

The new claims have been drafted so as not to be anticipated by SATO. SATO does not disclose the inventive system or method. More specifically, SATO does not disclose the recited

chaining key reception unit, chaining key decoding unit, and chaining key management unit.

Although SATO discusses decoding encrypted broadcasting signals, applicant does not see that SATO comprises the structure recited together with the recited chaining key management unit storing a series of chaining key and corresponding key identifier pairs. Nor is SATO seen to disclose a chaining key management unit configured to retrieve a previously-stored chaining key paired with a corresponding stored key identifier where the chaining key management unit receives a target key identifier and uses the target key identifier to extract from the stored pairs an appropriate chaining key to be sent to a decoding unit, wherein the decoding unit decodes the first chaining key using the retrieved chaining key (from the stored pairs in the memory) to generate a new chaining key.


Additionally, the details of the structure as recited by the dependent claims are not believed to be taught or suggested by SATO.

In summary, the claims are believed to be both novel and non-obvious over SATO and therefore their allowance is solicited.

The Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 25-0120 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17.

Respectfully submitted,

YOUNG & THOMPSON



Roland E. Long, Jr., Reg. No. 41,949
745 South 23rd Street
Arlington, VA 22202
Telephone (703) 521-2297
Telefax (703) 685-0573
(703) 979-4709

REL/lk

APPENDIX:

The Appendix includes the following items:

- amended abstract
- Replacement Sheets for Figures 4 and 5 of the drawings
- Figures A-C, as described above.